

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Satoshi INAMI et al. :
Serial No. NEW : **Attn: APPLICATION BRANCH**
Filed January 16, 2002 : **Attorney Docket No. 2002_0021A**
COMMUNICATIONS TERMINAL



CLAIM OF PRIORITY UNDER 35 USC 119

Assistant Commissioner for Patents,
Washington, DC 20231

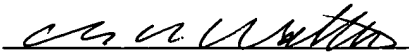
Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2001-011253, filed January 19, 2001, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Satoshi INAMI et al.

By 
Charles R. Watts
Registration No. 33,142
Attorney for Applicants

CRW/asd
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
January 16, 2002

日 本 国 特 許 庁
JAPAN PATENT OFFICE

J1050 U.S. PTO
10/046184
01/16/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2001年 1月19日

出 願 番 号
Application Number:

特願2001-011253

出 願 人
Applicant(s):

松下電器産業株式会社

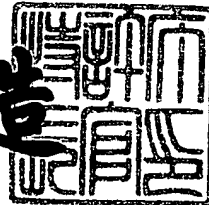
CERTIFIED COPY OF
PRIORITY DOCUMENT

BEST AVAILABLE COPY

2001年11月26日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3102474

【書類名】 特許願
【整理番号】 2037330001
【提出日】 平成13年 1月19日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 12/14
G06F 7/02

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 稲見 聡

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 水山 正重

【発明者】

【住所又は居所】 神奈川県横浜市港北区綱島東四丁目 3 番 1 号 松下通信
工業株式会社内

【氏名】 加藤 淳展

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 通信端末

【特許請求の範囲】

【請求項 1】サーバにアクセスし、データを送受信する通信端末であって、サーバとデータを送受信する通信部と、前記通信部が受信したデータを解析するファイル解析部と、前記ファイル解析部が解析したファイルからアプリケーションと認証情報とをとりだすアプリケーションインストール部と、アプリケーションを保存するアプリケーション保存部と、前記アプリケーションを起動するときに必要な認証に関する情報を保存するアプリケーション情報保存部と、前記ファイル解析部が解析した結果をもとに、どのアプリケーションを起動するかを判定し、アプリケーションを起動するアプリケーション起動部と、前記ファイル解析部が解析した結果、ファイルが認証を必要とする場合に認証処理を行う認証部とを備えたことを特徴とする通信端末。

【請求項 2】前記認証部は、前記通信端末内部に保持する認証データにより、受信したファイルを公開鍵暗号方式によって認証することを特徴とする請求項 1 記載の通信端末。

【請求項 3】前記認証部は、前記通信端末内部に保持する現在時刻データと、受信したファイルに書かれている有効期限情報との比較を行うことによって、認証することを特徴とする請求項 1 記載の通信端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信端末に関し、より特定的には、アプリケーションを組み込む時に、必要な認証の種別をアプリケーションと関連づけて保存しておき、アプリケーションを起動する場合に関連づけられている認証方法により認証を行う通信端末に関する。

【0002】

【従来の技術】

従来通信端末や携帯可能電子装置において、複数の認証レベルによりある特定

のデータに対するアクセスを許したり、ある条件の時に特定のアプリケーションを起動したりすることが行われている。

【0003】

かかる認証によりアクセスするアプリケーションを制限する手法の第1の方法が、特願昭62-503158に開示されている。第1の方法では、ユーザごとに複数のアクセス権限を定義し、そのアクセス権限によって、アクセスできるデータを判定している。

【0004】

また、第2の方法が、特願昭61-5722に開示されている。第2の方法では、アプリケーションを起動するかどうかは、端子にレベルの異なる信号を直接入力し、信号の比較により起動するかどうか決定していた。

【0005】

【発明が解決しようとする課題】

しかしながら、第1の方法では予めインストールされているアプリケーションごとに、アクセス権限が組み込まれてインストールされていて、アプリケーションは複雑なセキュリティを意識しつつ作成しなければならない。また、システムにアプリケーションを追加する場合、そのアプリケーションにアクセス制限のための手段を組み込んだ形でアプリケーションを作成し、インストールしなければならない。そのためアプリケーションは複雑で大きなものになってしまう。一方、認証処理を行い、成功した時にのみアプリケーションを起動するといったことは考えられていない。

【0006】

また、第2の方法では、アプリケーションを起動するかどうかの判別を、物理的な信号を端末に送信することによって行っている。そのため、あるファイルを読み込んだことを契機としてアプリケーションを起動するといったことは想定されていない。

【0007】

それゆえに本発明の目的は、通信端末にアプリケーションをインストールする場合に、アプリケーションを起動する場合の認証方式やアクセス制限のレベルを

サーバ主導で設定する仕組みを導入することで、インストールしたアプリケーションを起動する場合に、起動する契機となるファイルの種別と関連付けて設定された認証の方式やレベルにより、認証処理を行うことである。そうすることで、ユーザはアプリケーション起動時の負担が減少され、かつ、アプリケーションは複雑なアクセス制限についての負担を減少させることができる。

【0008】

【課題を解決するための手段】

上記目的を達成するために、本発明は、サーバにアクセスし、データを送受信する通信端末であって、サーバとデータを送受信する通信部と、前記通信部が受信したデータを解析するファイル解析部と、前記ファイル解析部が解析したファイルからアプリケーションと認証情報とをとりだすアプリケーションインストール部と、アプリケーションを保存するアプリケーション保存部と、前記アプリケーションを起動するときに必要な認証に関する情報を保存するアプリケーション情報保存部と、前記ファイル解析部が解析した結果からどのアプリケーションを起動するかを判定し、アプリケーションを起動するアプリケーション起動部と、前記ファイル解析部が解析した結果、ファイルが認証を必要とする場合に認証処理を行う認証部と、を有することを特徴とする通信端末である。

【0009】

【発明の実施の形態】

以下本発明の実施の形態について、図面を用いて詳細に説明する。図1は、本発明の実施の形態におけるシステム全体の構成を示す。

【0010】

本実施の形態において、コンテンツ取得システムは、サーバ11と、ネットワーク2と、通信端末31とから構成される。

【0011】

サーバ11は、いわゆるWWW (World Wide Web) サーバであって、図2に示すように、記憶装置111と、CPU112と、ROM113と、RAM114と、通信制御部115とを備えている。

【0012】

記憶装置 111 は、典型的にはハードディスクドライブからなり、少なくとも 1 つのプログラムデータ 116 と、一つのコンテンツ 117 を記憶している。プログラムデータ 116 は、通信端末がダウンロードしてインストールするプログラムと、プログラムについての情報からなるデータである。

【0013】

CPU 112 は、RAM 114 を作業領域として使いつつ、ROM 113 または記憶装置 111 に格納されたプログラムを実行する。

【0014】

通信端末 31 は、大略的には、図 3 に示すように、CPU 311 と、ROM 315 と、RAM 312 と、表示装置 313 と、入力装置 314 と、通信部 316 とを備えている。

【0015】

CPU 311 は、RAM 312 を作業領域として使いつつ、ROM 315 または、記憶装置に格納されたプログラムを実行する。図 3 は、プログラムが ROM 315 に保存されている場合を示している。

【0016】

入力装置 314 は、例えばキーボードから構成される。表示装置 313 は、例えば液晶ディスプレイで構成される。通信部 316 は、図 1 のネットワーク 2 を通じて通信を行う。

【0017】

次に、上記構成を有するアプリケーション組み込み方法を、図 4 のシーケンスチャートを参照して説明する。

【0018】

通信端末 31 の CPU 311 は、ユーザの操作を契機として、図 4 のシーケンスチャートに示される処理を開始する。

【0019】

まず、CPU 311 は、ユーザのコンテンツ選択によりネットワーク 2 にアクセスし、WWWサーバに対して選択されたコンテンツを要求する。ネットワークは有線であっても、無線であってもよい。(ステップ S1)。

【0020】

次に、送信要求は、ネットワーク2を経由して、サーバ11により受信される。サーバ11の通信制御部115は、ネットワーク2から受信した送信要求をCPU112に転送する。CPU112は、送信要求を受信すると、RAM114を作業領域として使いつつ、当該送信要求に含まれるURLから送信するプログラムデータ116を決定し、記憶装置111からプログラムデータ116を読み出し、通信制御部115に転送する。通信制御部115は、転送されたプログラムデータ116を、ネットワーク2に送出する（ステップS2）。

【0021】

サーバ11から送信されたデータは、ネットワーク2を経由して通信端末31の通信部316により受信される。その後、通信部316が受信したデータをRAM312に展開すると、CPU311は、ROM315にあるファイル解析部322を実行し、受信したプログラムデータ116の解析を行う。このときに受信するプログラムデータ116の具体例を図6に示す。プログラムデータ116には、インストールするアプリケーションデータ204の他は、アプリケーションデータ204を起動する場合に必要な認証の種別を示す認証タイプ202や、どのファイル種別のデータを読み込んだときにアプリケーションデータ204を起動するかを示すためのファイル種別203などを含んでいる。ファイル解析部は、プログラムデータ116の中からどの部分がそれぞれにあたるのかを判定する。（ステップS3）。

【0022】

次に、CPU311は、ROM315にあるアプリケーションインストール部323を実行し、アプリケーションデータ204をアプリケーション保存部326に保存する（ステップS4）。

【0023】

また、それ以外の認証タイプ202や、ファイル種別203をアプリケーション情報保存部327に保存する（ステップS5）。

【0024】

次に、上記構成を有するアプリケーションの起動方法を、図5のシーケンスチ

ャートを参照して説明する。

【0025】

通信端末31のCPU311は、ユーザの操作を契機として、図5のシーケンスチャートに示される処理を開始する。

【0026】

まず、CPU311は、ユーザのコンテンツ選択によりネットワーク2にアクセスし、WWWサーバに対して選択されたコンテンツを要求する。ネットワークは有線であっても、無線であってもよい（ステップS11）。

【0027】

次に、送信要求は、ネットワーク2を経由して、サーバ11により受信される。サーバ11の通信制御部115は、ネットワーク2から受信した送信要求をCPU112に転送する。CPU112は、送信要求を受信すると、RAM114を作業領域として使いながら、当該送信要求に含まれるURLから送信するコンテンツ117を決定し、記憶装置111からコンテンツ117を読み出し、通信制御部115に転送する。通信制御部115は、転送されたコンテンツデータを、ネットワーク2に送出する（ステップS12）。

【0028】

サーバ11から送信されたデータは、ネットワーク2を経由して通信端末31の通信部316により受信される。その後、通信部316が受信したデータをRAM312に展開すると、CPU311は、ROM315にあるファイル解析部322を実行し、受信したコンテンツ117の解析を行う。このときに受信するコンテンツ117の具体例を図7に示す。ここで示すコンテンツは、アプリケーションを起動する契機となる起動用データ401であるとする。起動用データ401には、アプリケーションが読み込むデータ402、秘密鍵で暗号化された署名403、公開鍵404からなる。ファイル解析部322は、起動用データ401の中からどの部分がそれぞれのデータにあたるのかを判定する。また、ファイル解析部は起動用データ401のファイル種別も判定する（ステップS13）。

【0029】

次に、CPU311は、ROM315にあるアプリケーション起動部324を

実行し、アプリケーション情報保存部327を参照しつつ、実行するアプリケーションを判定する。具体的には、アプリケーション情報保存部に保存されているファイル種別203と、受信したコンテンツ117のファイル種別を比較し、一致するファイル種別203が見つかった場合に、そのファイル種別と関連づけられて保存されているアプリケーションデータ204を決定する（ステップS14）。

【0030】

起動するアプリケーションが決定すると、そのアプリケーションが必要とする認証タイプをアプリケーション情報保存部327から読み出す。そして、その種別に基づき認証部325を用いて認証処理を行う。例えば認証種別が公開鍵による認証方式であり、コンテンツデータが図7に示すデータの場合、以下の手順により認証処理を行う。まず、データ402のハッシュ値をとる。次に、公開鍵404により秘密鍵で暗号化された署名403を復号化する。最後に、得られたハッシュ値と復号化された署名を比較し、一致した場合は、データ402は改ざんされていなくて正しいデータであると判断し、アプリケーション部326の起動処理を行う。アプリケーションは、表示装置313や入力装置314を利用してアプリケーションを実行する。一致しない場合は、データが改ざんされているため、データを破棄し処理をおわる（ステップS15）。

【0031】

以上の実施形態では、アプリケーションを起動する場合に必要な認証タイプは、プログラムデータ116に記述される認証タイプ202によって制御することができる。したがって、ユーザの選択によりアプリケーションをインストールすると、認証タイプも自動的に設定される。

【0032】

以上から明らかなように、本アプリケーション組み込みと起動方法によれば、アプリケーションを起動する場合の認証方式やアクセス制限のレベルを記述したファイルをサーバに用意しておくことで、インストールしたアプリケーションを起動する場合に、起動する契機となるファイルの種別と関連付けて設定された認証の方式やレベルにより、認証処理を行うことができるようになる。すなわち、

ユーザが通信端末にアプリケーションをインストールする際に、サーバ側主導で通信端末におけるアプリケーション実行時のセキュリティレベルをコントロールすることができる。

【0033】

なお、サーバで保持しているデータの形式の例として、ハイパーテキストの例をあげたが、具体的には、XML (eXtensible Markup Language) 形式やSGMLを用いて記述してもよい。あるいは、単にテーブルを用いて記述してもよい。

【0034】

なお、プログラムデータ116は、一つのファイルとして説明したが、認証タイプやファイル種別を別のファイルに記述し、アプリケーションデータを別個のファイルとしてインストール処理を行ってもよい。

【0035】

なお、認証タイプとしては、公開鍵暗号方式による方法を挙げたが、DES (Data Encryption Standard) など他の暗号方式を用いてもよい。

【0036】

【発明の効果】

以上のように本発明によれば、通信端末にアプリケーションをインストールする場合に、アプリケーションを起動する場合の認証方式やアクセス制限のレベルをサーバ主導で設定することができる。また、インストールしたアプリケーションを起動する場合に、起動する契機となるファイルの種別と関連付けられた認証の方式やレベルにより認証処理を行うことができるようにある。従って、ユーザは認証を行うための負担が減少し、アプリケーションは複雑なアクセス制限についての負担が減る。つまり、使いやすさとセキュリティを両立するアプリケーションを構築することが可能となる。

【図面の簡単な説明】

【図1】

本発明の実施の形態のアプリケーション組み込みと起動の方法を実現するシス

テムの構成を示すブロック図

【図 2】

本発明の実施の形態のサーバの構成を示すブロック図

【図 3】

本発明の実施の形態の通信端末の構成を示すブロック図

【図 4】

本発明の実施の形態の通信端末の処理手順を示すシーケンスチャート

【図 5】

本発明の実施の形態の通信端末の処理手順を示すシーケンスチャート

【図 6】

本発明の実施の形態の通信端末が使用するプログラムデータの具体例を示す図

【図 7】

本発明の実施の形態の通信端末が使用する起動用データの具体例を示す図

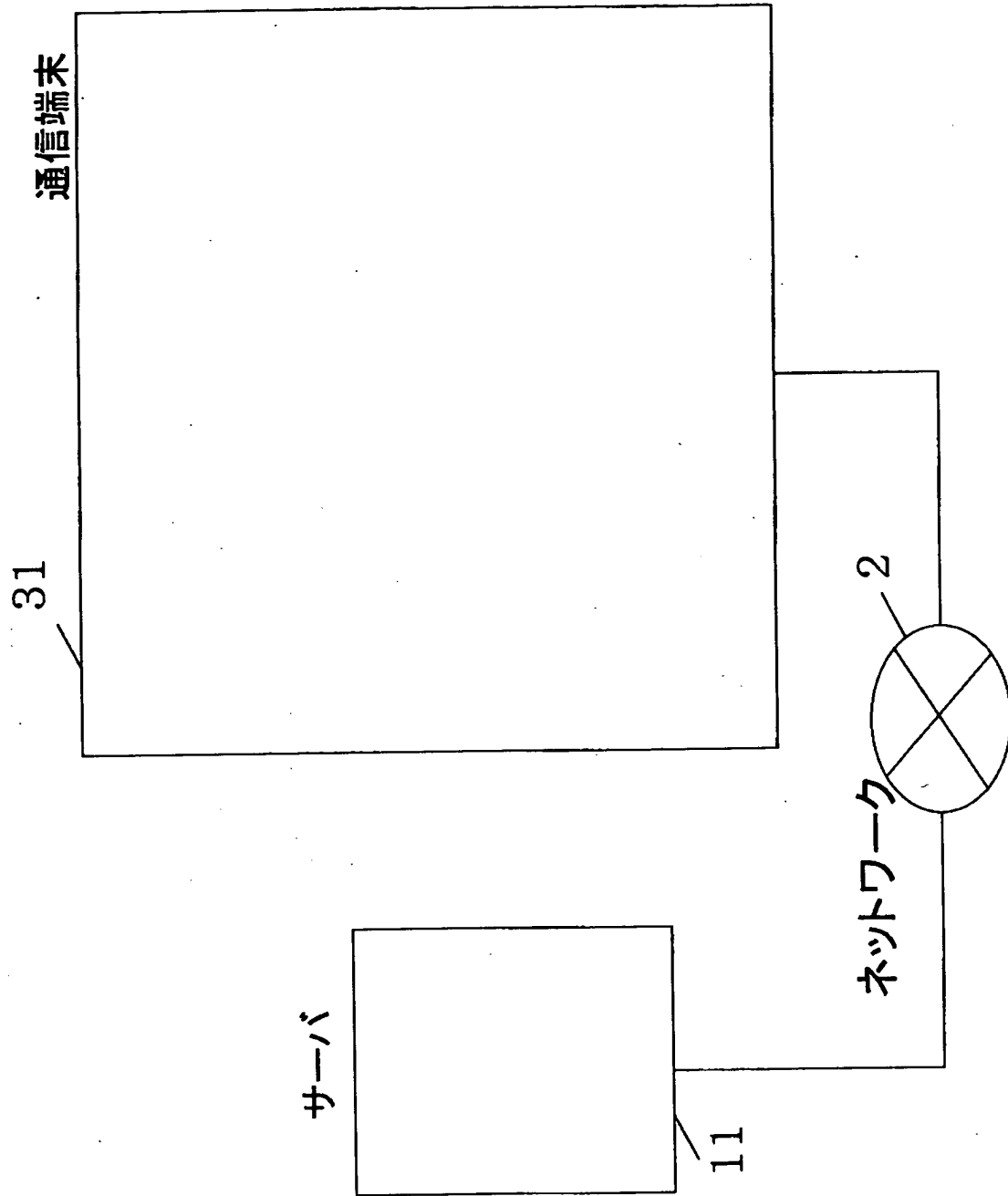
【符号の説明】

- 1 1 サーバ
- 2 ネットワーク
- 3 1 通信端末
- 3 2 2 ファイル解析部
- 3 2 3 アプリケーションインストール部
- 3 2 4 アプリケーション起動部
- 3 2 5 認証部
- 3 2 6 アプリケーション保存部
- 3 2 7 アプリケーション情報保存部
- 1 1 1 記憶装置
- 1 1 2 CPU
- 1 1 3 ROM
- 1 1 4 RAM
- 1 1 5 通信制御部
- 1 1 6 プログラムデータ

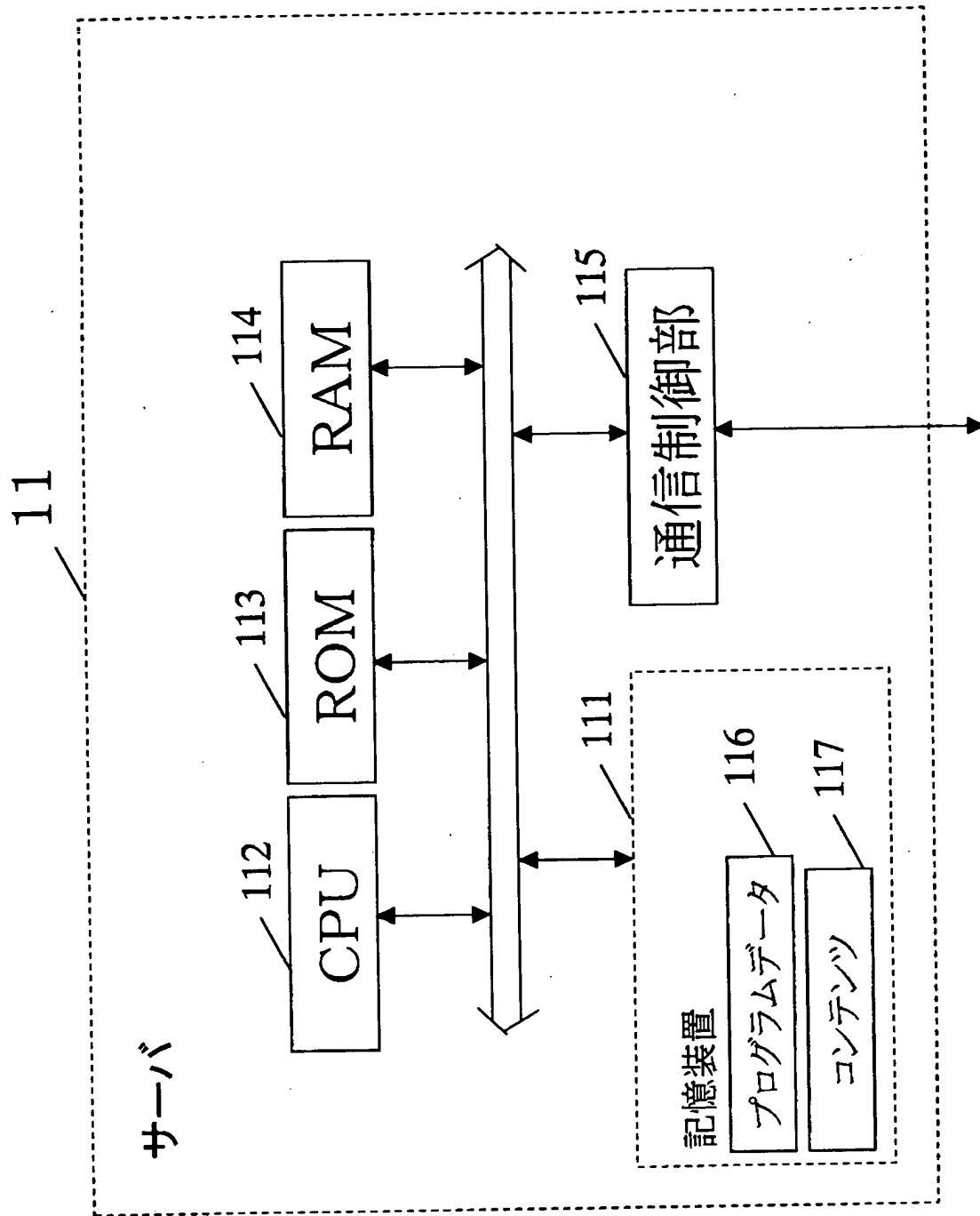
- 117 コンテンツ
- 311 CPU
- 312 RAM
- 313 表示装置
- 314 入力装置
- 315 ROM
- 316 通信部
- 202 認証タイプ
- 203 ファイル種別
- 204 アプリケーションデータ
- 401 起動用データ
- 402 データ
- 403 秘密鍵で暗号化された署名
- 404 公開鍵

【書類名】 図面

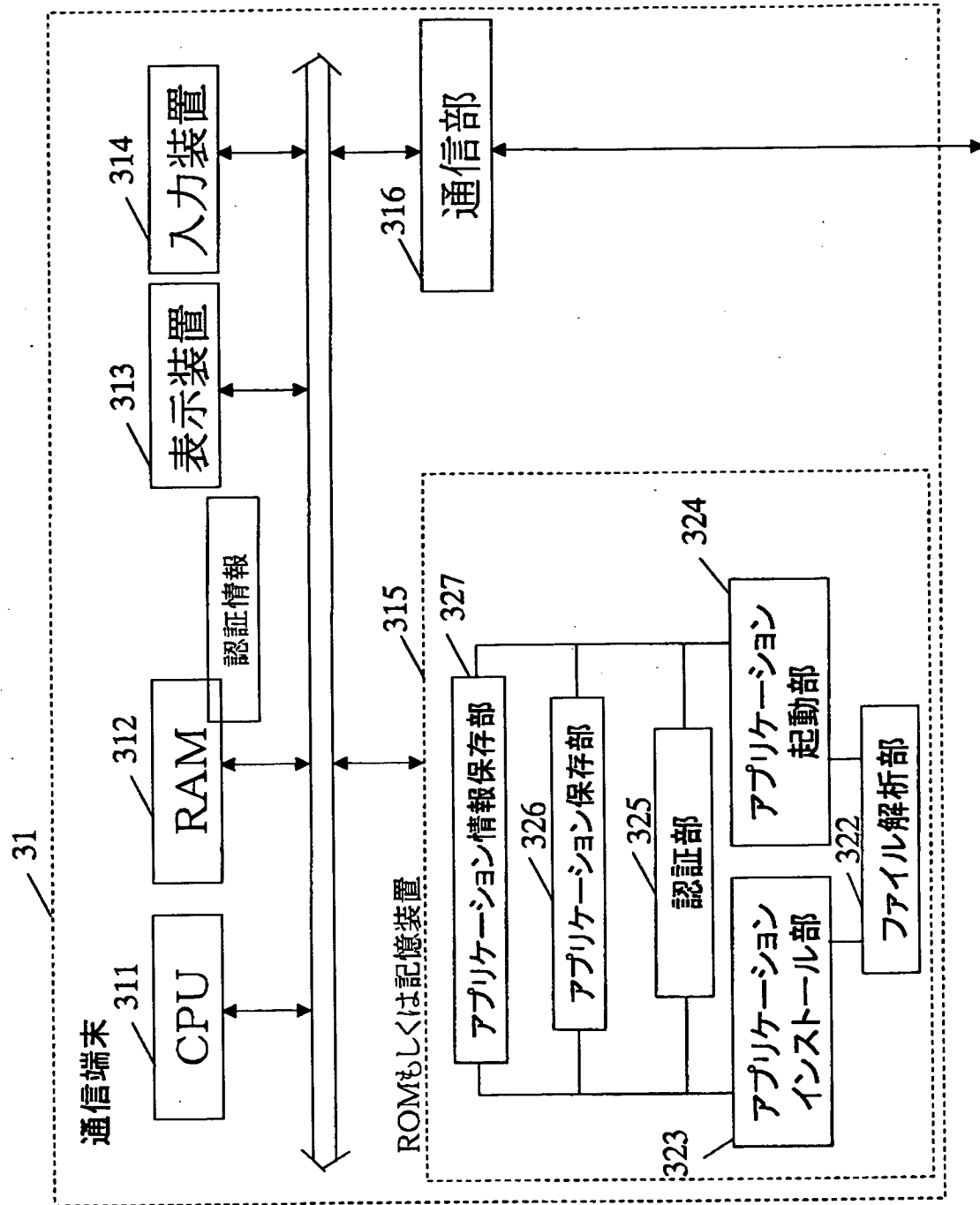
【図 1】



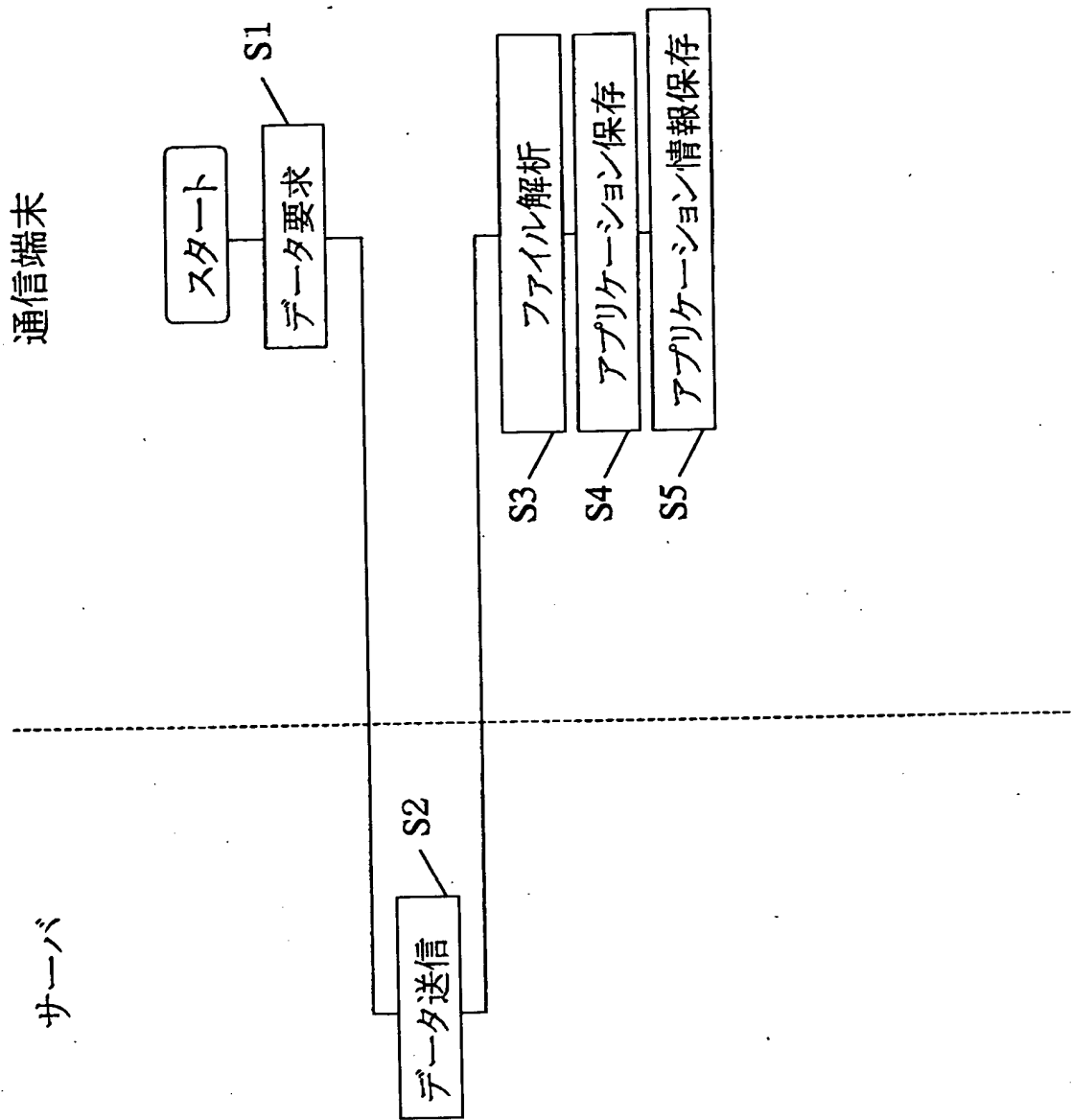
【図 2】



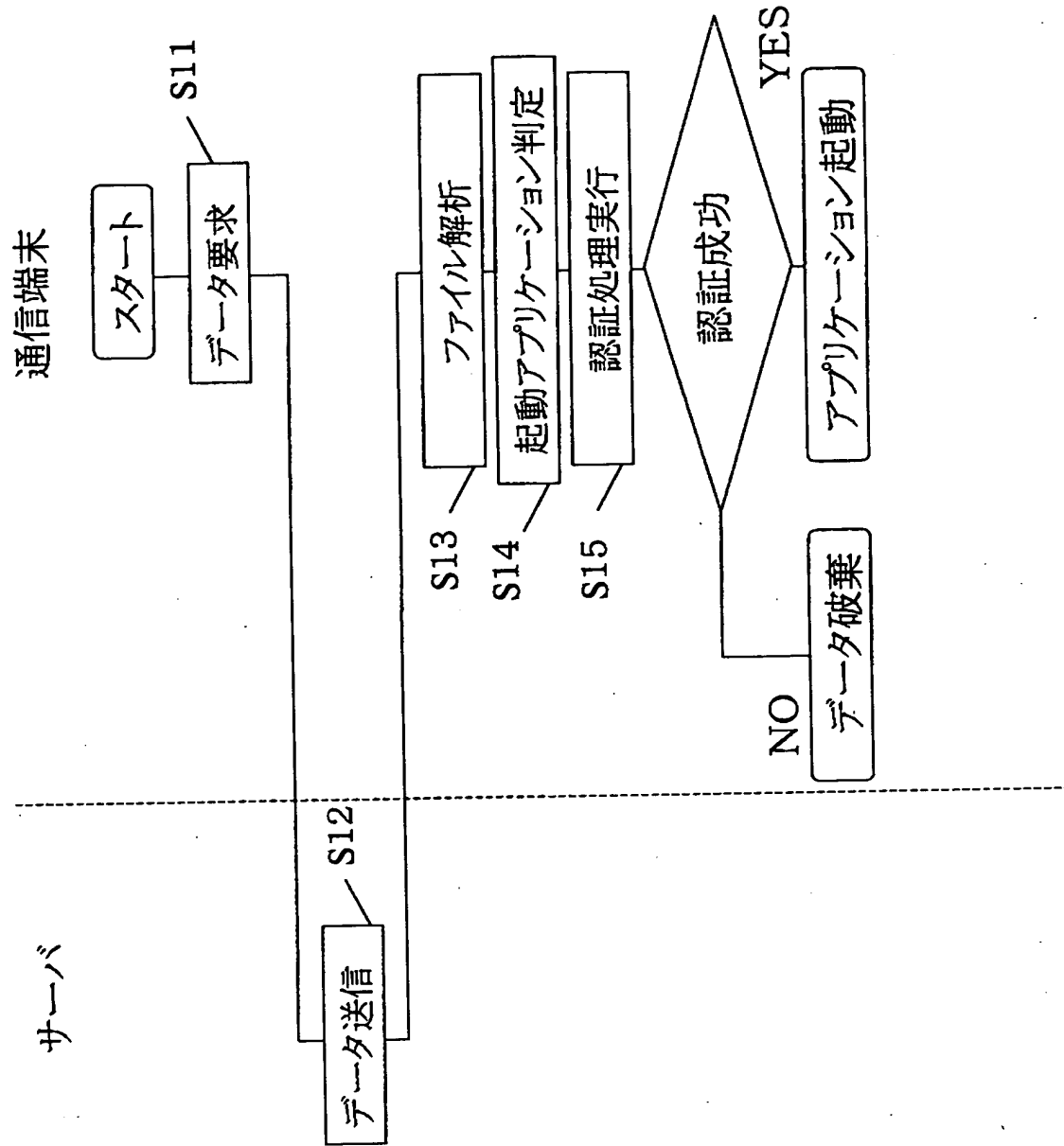
【図 3】



【図 4】



【図5】



【図 6】

プログラムデータ

116

<authType>	
認証タイプ	・ ・ 202
</authType>	
<fileType>	
ファイル種別	・ ・ 203
</fileType>	
<applicationData>	
アプリケーション・データ	・ ・ 204
</applicationData>	

【図 7】

起動用データ

401

<data> . . 402

データ

</data>

<signature>

秘密鍵で暗号化された署名 . . 403

</signature>

<certificate>

公開鍵 . . 404

</certificate>

【書類名】 要約書

【要約】

【課題】 アプリケーション起動時の認証タイプをアプリケーションとは独立に設定可能にしつつ、アプリケーションのインストール処理を自動的に行うことである。

【解決手段】 アプリケーションを保存しているサーバ11には、アプリケーション起動時の認証タイプを示すデータが保存されている。通信端末31はアプリケーションインストール時に、サーバ11から取得したデータを解析し、どの認証タイプかを判定し保存しておく。アプリケーション起動時にはその認証タイプ情報を読み込み、アプリケーション種別に基づく認証処理を行う。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社